EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	50	("5226055" "4835949" "3809141" "5479365" "6027973" "6228782" "6245090" "6504757" "5913399" "4274097" "5460933" "5758893" "6410213" "4322219" "5611434" "6292830" "6048416" "5521940" "6303929" "6436314" "6458294" "6471887" "4390987" "4599545" "4813217" "5379387" "5790139" "5970601" "3922246" "3903809" "3803734" "3793808" "4039625" "4050946" "4270137" "4333471" "4399292" "4478755" "4525565" "4609479" "4767108" "4775100" "4777338" "4788271" "4856223" "4894812" "4914491" "4915742" "4924614" "4954265").pn.	USPAT	OR	OFF	2006/05/17 16:42
S2	0	S1 and "finite field"	USPAT	OR	OFF	2005/09/09 14:46
S3	107	("5226055" "4835949" "3809141" "5479365" "6027973" "6228782" "6245090" "6504757" "5913399" "4274097" "5460933" "5758893" "6410213" "4322219" "5611434" "6292830" "6048416" "5521940" "6303929" "6436314" "6458294" "6471887" "4390987" "4599545" "4813217" "5379387" "5790139" "5970601" "3922246" "3903809" "3803734" "3793808" "4039625" "4050946" "4270137" "4333471" "4399292" "4478755" "4525565" "4609479" "4767108" "4775100" "4777338" "4788271" "4856223" "4894812" "4914491" "4915742" "4924614" "4954265").pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/09 14:46
S4	0	S3 and "finite field"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/09 14:47
S5	2	"6430588".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/09 14:51

EAST Search History

S6	410	"380"/$.ccls. and (elliptic with curve)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/09 14:53
S7	3	"380"/47.ccls. and (elliptic with curve)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/09 14:53
S8	167	"380"/$.ccls. and (elliptic with curve) and (finite adj field)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/09 14:53
S9	14	"380"/$.ccls. and (elliptic with curve) and ((finite adj field) with (multip$3))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/09 15:06
S10	2	"380"/$.ccls. and (elliptic with curve) and ((finite adj field) with (multip$3)) and (addition) and (accumulator$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/09 15:06
S11	164	380/47.ccls.	USPAT	OR	OFF	2005/09/13 11:16
S12	165	380/47.ccls.	US-PGPUB; USPAT	OR	OFF	2005/09/13 11:16
S13	180	380/47.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/13 11:16
S14	2	"6941311".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/05/16 17:29

EAST Search History

S15	50	("5226055" "4835949" "3809141" "5479365" "6027973" "6228782" "6245090" "6504757" "5913399" "4274097" "5460933" "5758893" "6410213" "4322219" "5611434" "6292830" "6048416" "5521940" "6303929" "6436314" "6458294" "6471887" "4390987" "4599545" "4813217" "5379387" "5790139" "5970601" "3922246" "3903809" "3803734" "3793808" "4039625" "4050946" "4270137" "4333471" "4399292" "4478755" "4525565" "4609479" "4767108" "4775100" "4777338" "4788271" "4856223" "4894812" "4914491" "4915742" "4924614" "4954265").pn.	USPAT	OR	OFF	2006/05/17 16:42
S16	0	S15 and (modular adj reduction$)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/05/17 16:43
S17	254	(modular adj reduction$)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/05/18 17:12
S18	1862	(finite adj field)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/05/18 17:12
S19	650	(finite adj field) same (addition subtraction multiplication division)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/05/18 17:57
S20	823	(finite adj field) same ((addition subtraction multiplication division) (add$3 subtract$3 multiply$3 divid$3))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/05/18 18:00

EAST Search History

S21	9	S20 same (modular$2 adj reduc$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/05/19 13:30
S22	175	380/47.ccls.	USPAT	OR	OFF	2006/05/19 19:28
S23	1491	380/28.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 18:39
S24	947	380/44.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 18:39
S25	861	713/171.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 18:39
S26	455	713/169.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 19:01
S27	3420	S23 S24 S25 S26	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 19:01
S28	287	S27 and (finite adj field)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:21
S29	311	S27 and (finite adj field)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/23 19:02

EAST Search History

S30	23	S27 and (finite adj field) and (accumulator$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/23 19:02
S31	43	S27 and (finite adj field) with (reduc$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/23 19:03
S32	40	S27 and (finite adj field) with (multipl$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/23 19:03
S33	2	S27 and (finite adj field) with (reduc$2) with (result$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/23 19:07
S34	350	S27 and (elliptic adj curve)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/23 19:08
S35	248	S27 and (elliptic adj curve) and (reduc$5)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/23 19:08
S36	7	S27 and (elliptic adj curve) and (reduc$5) and (word adj siz$4 with operation$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/23 20:27
S37	1491	380/28.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 20:28

EAST Search History

S38	947	380/44.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 20:28
S39	861	713/171.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 20:28
S40	455	713/169.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 20:28
S41	3420	S37 S38 S39 S40	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/23 20:28
S42	131	S41 and (modular$2 with reduc$5)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/23 20:28
S43	2	"20050071656"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/11/29 10:28
S44	1506	380/28.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:21
S45	956	380/44.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:21

EAST Search History

S46	876	713/171.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:21
S47	459	713/169.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:21
S48	3456	S44 S45 S46 S47	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:21
S49	3456	S48	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:21
S50	51	S48 and (reduction$2).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:24
S51	17	S48 and (reduction$2).clm. and (finite adj field$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:26
S52	8	S48 and (reduction$2).clm. and (finite adj field$2).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:30
S53	243	certicom.as.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:30

EAST Search History

S54	3	certicom.as. and (reduction$2).clm. and (finite adj field$2).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:31
S55	303	lambert near3 robert.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 17:31
S56	4	lambert near3 robert.in. and (reduction$2).clm. and (finite adj field$2).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/12/21 18:33

Terms used: finite field modular reduction

Found **12,286** of **216,199**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 A state-of-the-art elliptic curve cryptographic processor operating in the frequency domain

Selçuk Baktir, Sandeep Kumar, Christof Paar, Berk Sunar

August 2007 **Mobile Networks and Applications**, Volume 12 Issue 4

Publisher: ACM

Full text available: pdf(448.53 KB) Additional Information: full citation, abstract, references, index terms

We propose a novel area/time efficient elliptic curve cryptography (ECC) processor architecture which performs all finite field arithmetic operations in the discrete Fourier domain. The proposed architecture utilizes a class of optimal extension fields (OEF) $GF(q^m)$ where the field characteristic is a Mersenne prime $q = 2^n - 1$ and $m = n$. The main advantage of our architecture is that it achieves extension field modular multiplicat ...

Keywords: discrete Fourier domain, elliptic curve cryptography (ECC), finite fields, modular multiplication

2 Computing exact geometric predicates using modular arithmetic with single precision

Hervé Brönnimann, Ioannis Z. Emiris, Victor Y. Pan, Sylvain Pion

August 1997 **Proceedings of the thirteenth annual symposium on Computational geometry SCG '97**

Publisher: ACM Press

Full text available: pdf(1.28 MB) Additional Information: full citation, references, citings, index terms

Keywords: computational geometry, exact arithmetic, modular computations, residue number systems, robustness, single precision

3 Parallel exponentiators using data signal processor chips and transputers for a flexible and efficient software implementation of public-key cryptosystems to run on PC's or larger systems

Daniel Guinier

January 1989 **ACM SIGSAC Review**, Volume 6 Issue 4

Publisher: ACM Press

Full text available: pdf(688.36 KB) Additional Information: full citation, abstract, references, citings, index

terms

Algorithms for parallel computation (multiplication, reduction and exponentiation) over finite fields in the general case: GF(N) and where N is a Mersenne prime of 127, 521, 607 or 1279 bits: GF(2^p-1) are described. They find a direct application in the generation of asymmetric public-key cryptosystems.Two different ways are suggested to implement efficiently these algorithms:**The first** takes advantage of the RISC architecture of the transputers (INMOS IMS T414), the parallelism ...

4 High-level techniques for specific applications: High-level synthesis for large bit-width multipliers on FPGAs: a case study

Gang Quan, James P. Davis, Siddhaveerasharan Devarkal, Duncan A. Buell

September 2005 **Proceedings of the 3rd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '05 , Proceedings of the 3rd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '05**

Publisher: ACM Press, IEEE Computer Society

Full text available: pdf(427.32 KB) Publisher Site Additional Information: full citation, abstract, references, index terms

In this paper, we present the analysis, design and implementation of an estimator to realize large bit width unsigned integer multiplier units. Larger multiplier units are required for cryptography and error correction circuits for more secure and reliable transmissions over highly insecure and/or noisy channels in networking and multimedia applications. The design space for these circuits is very large when integer multiplication on large operands is carried out hierarchically. In this paper, w ...

Keywords: FPGA devices, design exploration, high level synthesis, large-scale integer multipliers, reconfigurable computing

5 Hardware organization to achieve high-speed elliptic curve cryptography for mobile devices

Sining Liu, Brian King, Wei Wang

August 2007 **Mobile Networks and Applications**, Volume 12 Issue 4

Publisher: ACM

Full text available: pdf(458.41 KB) Additional Information: full citation, abstract, references, index terms

Elliptic curve cryptography (ECC) is recognized as a fast cryptography system and has many applications in security systems. In this paper, a novel sharing scheme is proposed to significantly reduce the number of field multiplications and the usage of lookup tables, providing high speed operations for both hard-ware and software realizations.

Keywords: cryptographic hardware organization, elliptic curve cryptography, lookup table

6 Computer security and encryption I: Achieving efficient polynomial multiplication in fermat fields using the fast Fourier transform

Selçuk Baktir, Berk Sunar

March 2006 **Proceedings of the 44th annual Southeast regional conference ACM-SE 44**

Publisher: ACM Press

Full text available: pdf(190.68 KB) Additional Information: full citation, abstract, references, index terms

We introduce an efficient way of performing polynomial multiplication in a class of finite fields *GF(p^m)* in the frequency domain. The Fast Fourier Transform (FFT) based frequency domain multiplication technique, originally proposed for integer multiplication, provides an extremely efficient method for multiplication with the best known asymptotic complexity, i.e. $O(n \log n \log \log n)$. Unfortunately, the original FFT method bears significant overhead due to ...

Keywords: Fast Fourier Transform (FFT), coding theory, elliptic curve cryptography, fermat numbers, fermat transform, finite fields, polynomial multiplication

7 Security on FPGAs: State-of-the-art implementations and attacks
Thomas Wollinger, Jorge Guajardo, Christof Paar
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

8 Academic papers: Elliptic curve cryptography: Java implementation
Kossi D. Edoh
October 2004 **Proceedings of the 1st annual conference on Information security curriculum development InfoSecCD '04**
Publisher: ACM Press
Full text available: pdf(163.76 KB) Additional Information: full citation, abstract, references, index terms

The use of Java in developing commercial Internet applications is growing very rapidly. A major requirement for e-commerce applications is the provision of security. In this work we consider Elliptic Curve Cryptography (ECC) because of the high level of security it provides with small key sizes. ECC is ideal for use on constrained environments such as pagers, personal digital assistants, cellular phones and smart cards. We implement the ECC algorithms approved by the National Institute of Standa ...

Keywords: NIST, cryptography, elliptic curves, network security

9 Security: Attacking elliptic curve cryptosystems with special-purpose hardware
Tim Gueneysu, Christof Paar, Jan Pelzl
February 2007 **Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays FPGA '07**
Publisher: ACM Press
Full text available: pdf(198.70 KB) Additional Information: full citation, abstract, references, index terms

Since their invention in the mid 1980s, Elliptic Curve Cryptosystems (ECC) have become an alternative to common Public-Key (PK) cryptosystems such as, e.g., RSA. The utilization of Elliptic Curves (EC) in cryptography is very promising because of their

resistance against powerful index-calculus attacks. Providing a similar level of security as RSA, ECC allows for efficient implementation due to a significantly smaller bit size of the operands. It is widely accepted that the only feasible way to ...

Keywords: Pollard's Rho, cryptanalysis, discrete logarithm, elliptic curve cryptosystem

10 On the genericity of the modular polynomial GCD algorithm
Erich Kaltofen, Michael B. Monagan
July 1999 **Proceedings of the 1999 international symposium on Symbolic and algebraic computation ISSAC '99**
Publisher: ACM Press
Full text available: pdf(885.07 KB) Additional Information: full citation, references, citings, index terms

11 Recovery of algebraic numbers from their *p*-adic approximations
John Abbott
July 1989 **Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation ISSAC '89**
Publisher: ACM Press
Full text available: pdf(926.76 KB) Additional Information: full citation, abstract, references, index terms, review

We describe three ways to generalize Lenstra's algebraic integer recovery method. One direction adapts the algorithm so that rational numbers are automatically produced given only upper bounds on the sizes of the numerators and denominators. Another direction produces a variant which recovers algebraic numbers as elements of multiple generator algebraic number fields. The third direction explains how the method can work if a reducible minimal polynomial had been given for an algebraic gener ...

12 Security: CReconfigurable finite field instruction set architecture
Nathan Jachimie, Fernando Martinez-Vallin, Jafar Saniie
February 2007 **Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays FPGA '07**
Publisher: ACM Press
Full text available: pdf(236.94 KB) Additional Information: full citation, abstract, references, index terms

Reconfigurable computing can provide a significant speed-up factor to cryptographic and error correcting code algorithms. Finite field arithmetic is essential to both, but is difficult to implement efficiently. Finite field instruction set extensions and a reconfiguration framework have been constructed to enable a finite field multiplier to be regenerated via software control. A performance evaluation has been created by generating a Finite Field Extensions Unit with MicroBlaze processor in a X ...

Keywords: FSL, MicroBlaze, Xilinx, embedded development, fast simplex links, finite field arithmetic, galois fields, instruction set extensions, partial reconfiguration

13 Some results on theorem proving in geometry over finite fields
Dongdai Lin, Zhuojun Liu
August 1993 **Proceedings of the 1993 international symposium on Symbolic and algebraic computation ISSAC '93**
Publisher: ACM Press
Full text available: pdf(682.59 KB) Additional Information: full citation, references, index terms

14 Modular arithmetic and finite field theory: A tutorial
E. Horowitz
March 1971 **Proceedings of the second ACM symposium on Symbolic and algebraic manipulation SYMSAC '71**
Publisher: ACM Press
Full text available: pdf(569.15 KB) Additional Information: full citation, abstract, references, citings, index terms

The paradigm of algorithm analysis has achieved major pre-eminence in the field of symbolic and algebraic manipulation in the last few years. A major factor in its success has been the use of modular arithmetic. Application of this technique has proved effective in reducing computing times for algorithms covering a wide variety of symbolic mathematical problems. This paper is intended to review the basic theory underlying modular arithmetic. In addition, attention will be paid to certain pr ...

Keywords: Exact multiplication, Finite fields, Modular arithmetic, Symbol manipulation;

15 Riemann hypothesis and finding roots over finite fields
M-D A Huang
December 1985 **Proceedings of the seventeenth annual ACM symposium on Theory of computing STOC '85**
Publisher: ACM Press
Full text available: pdf(695.93 KB) Additional Information: full citation, abstract, references, citings, index terms

It is shown that assuming Generalized Riemann Hypothesis, the roots of $f(x) = 0$ mod p, where p is a prime and f(x) is an integral Abilene polynomial can be found in deterministic polynomial time. The method developed for solving this problem is also applied to prime decomposition in Abelian number fields, and the following result is obtained: assuming Generalized Riemann Hypotheses, for Abelian number ...

16 Interpolation of sparse multivariate polynomials over large finite fields with applications
Ming-Deh A. Huang, Ashwin J. Rao
January 1996 **Proceedings of the seventh annual ACM-SIAM symposium on Discrete algorithms SODA '96**
Publisher: Society for Industrial and Applied Mathematics
Full text available: pdf(1.19 MB) Additional Information: full citation, references, citings, index terms

17 Finite field manipulations in Macsyma
K. T. Rowney, R. D. Silverman
January 1989 **ACM SIGSAM Bulletin**, Volume 23 Issue 1
Publisher: ACM Press
Full text available: pdf(622.33 KB) Additional Information: full citation, abstract, references, index terms

We present the implementation of an extensive system of routines, in Macsyma, which allows finite field arithmetic and manipulation of symbolic objects in finite fields,

18 Searching for primitive roots in finite fields
V. Shoup
April 1990 **Proceedings of the twenty-second annual ACM symposium on Theory of computing STOC '90**
Publisher: ACM Press

Full text available: pdf(649.12 KB) Additional Information: full citation, citings, index terms

19 Multiplicative complexity of polynomial multiplication over finite fields
Michael Kaminski, Nader H. Bshouty
January 1989 **Journal of the ACM (JACM)**, Volume 36 Issue 1
Publisher: ACM Press

Full text available: pdf(1.60 MB) Additional Information: full citation, abstract, references, index terms, review

Let Mq(n) denote the number of multiplications required to compute the coefficients of the product of two polynomials of degree n over a q-element field by means of bilinear algorithms. It is shown that Mq(n) ≱ 3n - o(n). In particular, if q/2 < n ⪇

20 The parallel complexity of exponentiating polynomials over finite fields
Faith E. Fich, Martin Tompa
June 1988 **Journal of the ACM (JACM)**, Volume 35 Issue 3
Publisher: ACM Press

Full text available: pdf(1.14 MB) Additional Information: full citation, abstract, references, index terms, review

Modular integer exponentiation (given a, e, and m, compute ae mod m) is a fundamental problem in algebraic complexity for which no efficient parallel algorithm is known. Two closely related problems are modular polynomial exponentiation (given a(x), e, and m(x), compute (a(x)) ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Terms used: **finite field** **modular reduction**

Found **597** of **216,199**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 A state-of-the-art elliptic curve cryptographic processor operating in the frequency domain

Selçuk Baktir, Sandeep Kumar, Christof Paar, Berk Sunar

August 2007 **Mobile Networks and Applications**, Volume 12 Issue 4

Publisher: ACM

Full text available: pdf(448.53 KB) Additional Information: full citation, abstract, references, index terms

We propose a novel area/time efficient elliptic curve cryptography (ECC) processor architecture which performs all finite field arithmetic operations in the discrete Fourier domain. The proposed architecture utilizes a class of optimal extension fields (OEF) *GF* (q^m) where the field characteristic is a Mersenne prime $q = 2^n - 1$ and $m = n$. The main advantage of our architecture is that it achieves extension field modular multiplicat ...

Keywords: discrete Fourier domain, elliptic curve cryptography (ECC), finite fields, modular multiplication

2 Computing exact geometric predicates using modular arithmetic with single precision

Hervé Brönnimann, Ioannis Z. Emiris, Victor Y. Pan, Sylvain Pion

August 1997 **Proceedings of the thirteenth annual symposium on Computational geometry SCG '97**

Publisher: ACM Press

Full text available: pdf(1.28 MB) Additional Information: full citation, references, citings, index terms

Keywords: computational geometry, exact arithmetic, modular computations, residue number systems, robustness, single precision

3 Parallel exponentiators using data signal processor chips and transputers for a flexible and efficient software implementation of public-key cryptosystems to run on PC's or larger systems

Daniel Guinier

January 1989 **ACM SIGSAC Review**, Volume 6 Issue 4

Publisher: ACM Press

Full text available: pdf(688.36 KB) Additional Information: full citation, abstract, references, citings, index

terms

Algorithms for parallel computation (multiplication, reduction and exponentiation) over finite fields in the general case: GF(N) and where N is a Mersenne prime of 127, 521, 607 or 1279 bits: GF(2^p-1) are described. They find a direct application in the generation of asymmetric public-key cryptosystems.Two different ways are suggested to implement efficiently these algorithms:**The first** takes advantage of the RISC architecture of the transputers (INMOS IMS T414), the parallelism ...

4 High-level techniques for specific applications: High-level synthesis for large bit-width multipliers on FPGAs: a case study
Gang Quan, James P. Davis, Siddhaveerasharan Devarkal, Duncan A. Buell
September 2005 **Proceedings of the 3rd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '05 , Proceedings of the 3rd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '05**
Publisher: ACM Press, IEEE Computer Society
Full text available: pdf(427.32 KB) Publisher Site Additional Information: full citation, abstract, references, index terms

In this paper, we present the analysis, design and implementation of an estimator to realize large bit width unsigned integer multiplier units. Larger multiplier units are required for cryptography and error correction circuits for more secure and reliable transmissions over highly insecure and/or noisy channels in networking and multimedia applications. The design space for these circuits is very large when integer multiplication on large operands is carried out hierarchically. In this paper, w ...

Keywords: FPGA devices, design exploration, high level synthesis, large-scale integer multipliers, reconfigurable computing

5 Hardware organization to achieve high-speed elliptic curve cryptography for mobile devices
Sining Liu, Brian King, Wei Wang
August 2007 **Mobile Networks and Applications**, Volume 12 Issue 4
Publisher: ACM
Full text available: pdf(458.41 KB) Additional Information: full citation, abstract, references, index terms

Elliptic curve cryptography (ECC) is recognized as a fast cryptography system and has many applications in security systems. In this paper, a novel sharing scheme is proposed to significantly reduce the number of field multiplications and the usage of lookup tables, providing high speed operations for both hard-ware and software realizations.

Keywords: cryptographic hardware organization, elliptic curve cryptography, lookup table

6 Security on FPGAs: State-of-the-art implementations and attacks
Thomas Wollinger, Jorge Guajardo, Christof Paar
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

7 Academic papers: Elliptic curve cryptography: Java implementation
Kossi D. Edoh
October 2004 **Proceedings of the 1st annual conference on Information security curriculum development InfoSecCD '04**
Publisher: ACM Press
Full text available: pdf(163.76 KB) Additional Information: full citation, abstract, references, index terms

The use of Java in developing commercial Internet applications is growing very rapidly. A major requirement for e-commerce applications is the provision of security. In this work we consider Elliptic Curve Cryptography (ECC) because of the high level of security it provides with small key sizes. ECC is ideal for use on constrained environments such as pagers, personal digital assistants, cellular phones and smart cards. We implement the ECC algorithms approved by the National Institute of Standa ...

Keywords: NIST, cryptography, elliptic curves, network security

8 Security: Attacking elliptic curve cryptosystems with special-purpose hardware
Tim Gueneysu, Christof Paar, Jan Pelzl
February 2007 **Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays FPGA '07**
Publisher: ACM Press
Full text available: pdf(198.70 KB) Additional Information: full citation, abstract, references, index terms

Since their invention in the mid 1980s, Elliptic Curve Cryptosystems (ECC) have become an alternative to common Public-Key (PK) cryptosystems such as, e.g., RSA. The utilization of Elliptic Curves (EC) in cryptography is very promising because of their resistance against powerful index-calculus attacks. Providing a similar level of security as RSA, ECC allows for efficient implementation due to a significantly smaller bit size of the operands. It is widely accepted that the only feasible way to ...

Keywords: Pollard's Rho, cryptanalysis, discrete logarithm, elliptic curve cryptosystem

9 Computer security and encryption I: Achieving efficient polynomial multiplication in fermat fields using the fast Fourier transform
Selçuk Baktir, Berk Sunar
March 2006 **Proceedings of the 44th annual Southeast regional conference ACM-SE 44**
Publisher: ACM Press
Full text available: pdf(190.68 KB) Additional Information: full citation, abstract, references, index terms

We introduce an efficient way of performing polynomial multiplication in a class of finite fields $GF(p^m)$ in the frequency domain. The Fast Fourier Transform (FFT) based frequency domain multiplication technique, originally proposed for integer multiplication, provides an extremely efficient method for multiplication with the best known asymptotic complexity,

i.e. $O(n \log n \log \log n)$. Unfortunately, the original FFT method bears significant overhead due to ...

Keywords: Fast Fourier Transform (FFT), coding theory, elliptic curve cryptography, fermat numbers, fermat transform, finite fields, polynomial multiplication

10 On the genericity of the modular polynomial GCD algorithm
Erich Kaltofen, Michael B. Monagan
July 1999 **Proceedings of the 1999 international symposium on Symbolic and algebraic computation ISSAC '99**
Publisher: ACM Press
Full text available: pdf(885.07 KB) Additional Information: full citation, references, citings, index terms

11 Multiplication of large integers by the use of modular arithmetic: application to cryptography
Daniel Guinier
January 1990 **ACM SIGSAC Review**, Volume 7 Issue 4
Publisher: ACM Press
Full text available: pdf(692.11 KB) Additional Information: full citation, abstract, references, citings, index terms

Computing the long multiplication in fixed-radix representation is described first which suggests the use of two mixed solutions: first the sequentialisation of Karatsuba's algorithm by its extension to hexa and octo-mul then their judicious combination plus Implementation in Occam 2 language.**Computing the long multiplication in modular representation**. Including the principles of modular arithmetic and the *Chinese remainder* theorem, with efficient methods, is given in detail ...

12 A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes
Rodrigo Roman, Cristina Alcaraz, Javier Lopez
August 2007 **Mobile Networks and Applications**, Volume 12 Issue 4
Publisher: ACM
Full text available: pdf(468.79 KB) Additional Information: full citation, abstract, references, index terms

In a wireless sensor network environment, a sensor node is extremely constrained in terms of hardware due to factors such as maximizing lifetime and minimizing physical size and overall cost. Nevertheless, these nodes must be able to run cryptographic operations based on primitives such as hash functions, symmetric encryption and public key cryptography in order to allow the creation of secure services. Our objective in this paper is to survey how the existing research-based and commercial-ba ...

Keywords: cryptography, hardware, sensor networks

13 Recovery of algebraic numbers from their *p*-adic approximations
John Abbott
July 1989 **Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation ISSAC '89**
Publisher: ACM Press
Full text available: pdf(926.76 KB) Additional Information: full citation, abstract, references, index terms, review

We describe three ways to generalize Lenstra's algebraic integer recovery method. One

direction adapts the algorithm so that rational numbers are automatically produced given only upper bounds on the sizes of the numerators and denominators. Another direction produces a variant which recovers algebraic numbers as elements of multiple generator algebraic number fields. The third direction explains how the method can work if a reducible minimal polynomial had been given for an algebraic gener ...

14 Regular contributions: Architectural tradeoff in implementing RSA processors
Fu-Chi Chang, Chia-Jiu Wang
March 2002 **ACM SIGARCH Computer Architecture News**, Volume 30 Issue 1
Publisher: ACM Press
Full text available: pdf(385.39 KB) Additional Information: full citation, abstract, references, index terms

An investigation of a suite of RSA processors using different exponentiation and modular arithmetic algorithms is the main theme of this paper. The execution time and the amount of hardware required of different algorithms used to implement the RSA processor are compared. The modular algorithms examined in this paper are classical modular algorithm, Barrett's modular algorithm, Hensel's odd division and Montgomery's modular algorithm. The exponentiation algorithms implemented are the left-to-rig ...

15 On the hardness of computing the permanent of random matrices (extended abstract)
Uriel Feige, Carsten Lund
July 1992 **Proceedings of the twenty-fourth annual ACM symposium on Theory of computing STOC '92**
Publisher: ACM Press
Full text available: pdf(1.18 MB) Additional Information: full citation, abstract, references, citings, index terms

We study the complexity of computing the permanent on random inputs. We consider matrices drawn randomly from the space of n by n matrices with integer values between 0 and p−1, for any large enough prime p. We show that any polynomial time algorithm which computes the permanent correctly on even an exponentially small fraction of these matrices, implies the collapse of the polynomial-time hierarchy to its second leve ...

16 Factoring and decomposing ore polynomials over $F_q(t)$
Mark Giesbrecht, Yang Zhang
August 2003 **Proceedings of the 2003 international symposium on Symbolic and algebraic computation ISSAC '03**
Publisher: ACM Press
Full text available: pdf(281.17 KB) Additional Information: full citation, abstract, references, citings, index terms

We present algorithms for computing factorizations and least common left multiple (LCLM) decompositions of Ore polynomials over **F**$q(t)$, for a prime power $q=p^{\mu}$. Our algorithms are effective in **F**$q(t)[D;\sigma,\delta]$, for any automorphism σ and σ-derivation δ of **F**$q(t)$. On input $f \in$ **F**$q(t)[D;\sigma,\delta]$, the algorithms r ...

Keywords: eigenring, factoring, modular, ore polynomial

17 Security: CReconfigurable finite field instruction set architecture
Nathan Jachimie, Fernando Martinez-Vallin, Jafar Saniie
February 2007 **Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays FPGA '07**
Publisher: ACM Press
Full text available: pdf(236.94 KB) Additional Information: full citation, abstract, references, index terms

Reconfigurable computing can provide a significant speed-up factor to cryptographic and error correcting code algorithms. Finite field arithmetic is essential to both, but is difficult to implement efficiently. Finite field instruction set extensions and a reconfiguration framework have been constructed to enable a finite field multiplier to be regenerated via software control. A performance evaluation has been created by generating a Finite Field Extensions Unit with MicroBlaze processor in a X ...

Keywords: FSL, MicroBlaze, Xilinx, embedded development, fast simplex links, finite field arithmetic, galois fields, instruction set extensions, partial reconfiguration

18 Some results on theorem proving in geometry over finite fields
Dongdai Lin, Zhuojun Liu
August 1993 **Proceedings of the 1993 international symposium on Symbolic and algebraic computation ISSAC '93**
Publisher: ACM Press
Full text available: pdf(682.59 KB) Additional Information: full citation, references, index terms

19 Modular arithmetic and finite field theory: A tutorial
E. Horowitz
March 1971 **Proceedings of the second ACM symposium on Symbolic and algebraic manipulation SYMSAC '71**
Publisher: ACM Press
Full text available: pdf(569.15 KB) Additional Information: full citation, abstract, references, citings, index terms

The paradigm of algorithm analysis has achieved major pre-eminence in the field of symbolic and algebraic manipulation in the last few years. A major factor in its success has been the use of modular arithmetic. Application of this technique has proved effective in reducing computing times for algorithms covering a wide variety of symbolic mathematical problems. This paper is intended to review the basic theory underlying modular arithmetic. In addition, attention will be paid to certain pr ...

Keywords: Exact multiplication, Finite fields, Modular arithmetic, Symbol manipulation;

20 Interpolation of sparse multivariate polynomials over large finite fields with applications
Ming-Deh A. Huang, Ashwin J. Rao
January 1996 **Proceedings of the seventh annual ACM-SIAM symposium on Discrete algorithms SODA '96**
Publisher: Society for Industrial and Applied Mathematics
Full text available: pdf(1.19 MB) Additional Information: full citation, references, citings, index terms

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next